RDX 32

EXHIBIT NO. 6
Gieron
5-4-10
jmsteno.com

CC Numbers by Account

85658	AMERICANEXPRESS	374484363001003	06/06	M D	PO Box 54838	Manama	WA	BHR	54838
86553	VISA	4919936007928804	10/06	Marc Cohen	1516 Running Oak Lane	Royal Palm Beach	FL	USA	33411
87011	AMERICANEXPRESS	374484363001003	06/06	M D	PO Box 54838	Manama		BHR	54838
87056	AMERICANEXPRESS	374484363001003	06/06	M D	PO Box 54838	Manama		BHR	54838
87129	AMERICANEXPRESS	374484363001003	06/08	M D	po box 54838	manama		BHR	54838
87712	AMERICANEXPRESS	374484363001003	06/08	M D	po box 54838	manama		BHR	54838
88639	AMERICANEXPRESS	374484363001003	06/08	M D	po box 54838	manama		BHR	54838
88726	AMERICANEXPRESS	374484363001003	06/06	M D	PO Box 54838	Manama		BHR	54838
89573	AMERICANEXPRESS	374484363001003	06/06	M D	PO Box 54838	Manama		BHR	54838
89923	VISA	4085860000288883	04/07	M Dsouza	22 Carnegie Cres	Thornhill	OT	USA	l3t5h1
90012	AMERICANEXPRESS	374484363001003	06/06	m d	po box 54838	manama		BHR	54838
90396	AMERICANEXPRESS	374484363001003	06/06	M D	PO Box 54838	Manama		BHR	54838
90448	AMERICANEXPRESS	374484363001003	06/06	M D	PO Box 54838	Manama		BHR	54838
90729	AMERICANEXPRESS	374484363001003	06/06	M D	PO Box 54838	Manama		BHR	54838
90979	AMERICANEXPRESS	374484363001003	06/06	M D	PO Box 54838	Manama		BHR	54838
90980	AMERICANEXPRESS	374484363001003	06/06	M D	PO Box 54838	Manama		BHR	54838
90981	AMERICANEXPRESS	374484363001003	06/06	M D	PO Box 54838	Manama		BHR	54838
90982	AMERICANEXPRESS	374484363001003	06/06	M D	PO Box 54838	Manama		BHR	54838
500140	AMERICANEXPRESS	374484363001003	06/06	M D	PO Box 54838	Manama		BHR	54838
511143	AMERICANEXPRESS	374484363001003	06/06	M D	PO Box 54838	Manama		BHR	54838
516308	AMERICANEXPRESS	374484363001003	06/06	M D	PO Box 54838	Manama		BHR	54838
553971	AMERICANEXPRESS	374484363001003	06/08	M D	PO Box 54838	Manama		BHR	54838
554472	AMERICANEXPRESS	374484363001003	06/08	M D	PO Box 54838	Manama		BHR	54838
554990	AMERICANEXPRESS	374484363001003	06/08	M D	PO Box 54838	Manama		BHR	54838
554992	AMERICANEXPRESS	374484363001003	06/08	M D	PO Box 54838	Manama		BHR	54838
554994	AMERICANEXPRESS	374484363001003	06/08	M D	po box 54838	manama		BHR	54838
554995	AMERICANEXPRESS	374484363001003	06/08	M D	po box 54838	manama		BHR	54838
555192	VISA	4426217015787003	03/10	Daniel Sundin	300 lenora street	seattle	WA	USA	98121
555466	AMERICANEXPRESS	374484363001003	06/08	M D	PO Box 54838	Manama		BHR	54838
555630	AMERICANEXPRESS	374484363001003	06/08	M D	po box 54838	manama	OT	BHR	54838
555632	AMERICANEXPRESS	374484363001003	06/08	M D	po box 54838	manama	OT	BHR	54838
555633	AMERICANEXPRESS	374484363001003	06/08	M D	po box 54838	manama	OT	BHR	54838
555634	AMERICANEXPRESS	374484363001003	06/08	M D	po box 54838	manama	OT	USA	54838
555635	AMERICANEXPRESS	374484363001003	06/08	M.D	po box 54838	manama	OT	BHR	54838
555636	VISA	4426217015787003	03/10	Daniel Sundin	300 lenora street	Seattle	WA	USA	98121
555660	AMERICANEXPRESS	374484363001003	06/08	M D	po box 54838	manama	OT	BHR	54838
555662	AMERICANEXPRESS	374484363001003	06/08	M D	po box 54838	manama	OT	BHR	54838
555664	AMERICANEXPRESS	374484363001003	06/08	M D	po box 54838	manama	OT	BHR	54838
555665	AMERICANEXPRESS	374484383001003	06/08	M D	po box 54838	manama	OT	BHR	54838
557556	AMERICANEXPRESS	374484363001003	06/08	M D	PO Box 54838	Manama		BHR	54838

CC Numbers by Account

558332	AMERICANEXPRESS	374484363001003	08/08	M D	po box 54838	Manama	OT	BHR	54838
558333	AMERICANEXPRESS	374484363001003	02/08	M D	po box 54838	Manama	OT	BHR	54838
558334	AMERICANEXPRESS	374484363001003	02/08	M D	po box 54838	Manama	OT	BHR	54838
558335	AMERICANEXPRESS	374484363001003	02/08	M D	po box 54838	Manama	OT	BHR	54838
558336	AMERICANEXPRESS	374484363001003	02/08	M D	po box 54838	Manama	OT	BHR	54838
558337	AMERICANEXPRESS	374484363001003	02/08	M D	po box 54838	Manama	OT	BHR	54838
558338	AMERICANEXPRESS	374484363001003	02/08	M D	po box 54838	Manama	OT	BHR	54838

RDX 33

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

Ethan Arenson
Attorney
Division of Marketing Practices

Direct Dial 202-326-2204
Fax 202-326-3395
E-mail earenson@ftc.gov

February 22, 2010

VIA ELECTRONIC MAIL AND FIRST CLASS MAIL

Dan Webb
Thomas L. Kirsch
Winston & Strawn LLP
35 West Wacker Drive
Chicago, IL 60601-9703

Carolyn Gurland
2731 N. Mildred Avenue
Chicago, IL 60614

Garret Rasmussen
Orrick
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706

Re: FTC v. Innovative Marketing, Inc. et al.
RDB 08-CV-3233 (D. Md. 2008)

Dear Counsel:

Pursuant to Fed. R. Civ. Pro. 26(a)(2), and the scheduling order entered in the above-captioned case, enclosed please find the expert report of Kevin Johnson.

Sincerely,

Ethan Arenson

CERTIFICATE OF SERVICE

I hereby certify that on February 22, 2010, I caused a true and correct copy of the foregoing 26(a)(2) disclosure and accompanying Expert Report of Kevin Johnson to be served via electronic mail and first class mail, postage pre-paid, upon the following:

Tom Kirsch
Dan Webb
Winston & Strawn
35 W. Wacker Drive
Chicago, Illinois
60601-9703

Carolyn Gurland
2731 N. Mildred Avenue
Chicago, IL 60614

Counsel for Kristy Ross

Garret Rasmussen
Michael Madigan
Orrick
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706

Counsel for Marc and Maurice D'Souza

/s/ Ethan Arenson
Ethan Arenson

Expert Report of Kevin Johnson

Introduction

In December of 2009, I was asked by the Federal Trade Commission to review various graphics, Adobe Flash objects and Windows binaries. This review was to focus on what actions the advertising and binaries were performing and if these actions actually detected malware on the client machines.

I approached this examination as three distinct tasks. First I evaluated the graphic files, followed by examining the Flash objects and finally I ran the Windows binaries to determine their actions and effectiveness.

Qualifications

I am a Senior Security Analyst with InGuardians. I have a background in security from a development and system administration background. I have 13 years of experience performing security services for Fortune 100 companies and in my spare time contribute to a large number of open source security projects.

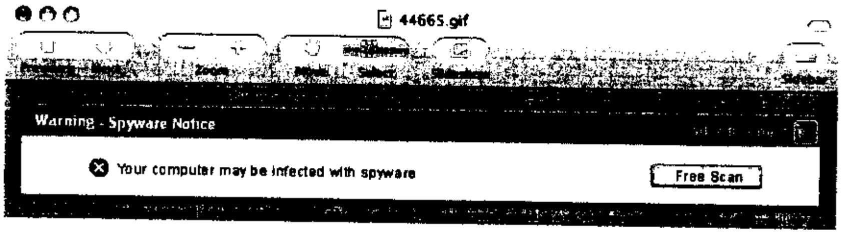
I founded and lead the development of B.A.S.E. (the Basic Analysis and Security Engine) project. The BASE project is the most popular web interface for the Snort intrusion detection system. I am also a faculty member at the SANS Technology Institute where I both teach the Incident Handling and Hacker Techniques class and am the author of the web application pen-testing class Sec542. SANS is one of the most trusted sources for computer security training. I have presented on many computer security topics to many organizations, including Infragard, ISACA, ISSA and the University of Florida. These presentations include Flash and web security topics. Other then Sec542 and various PowerPoint presentations, I have not authored any publications in the last 10 years nor have I testified as an expert at trial or deposition in the last 4 years.

For further information regarding my qualifications, please see my resume attached as Exhibit 1. The Federal Trade Commission is paying InGuardians a rate of 200 dollars per hour for compensation; this payment is not contingent on the outcome of our analysis.

Testing and analysis

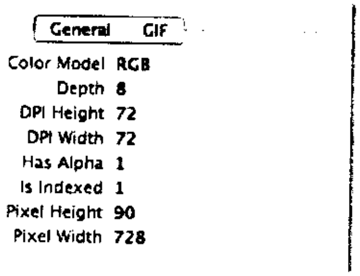
Beginning with the graphic files, I was provided from the FTC a CD of web files as well as a list of graphics that had over 500,000 impressions in the web logs. A list of these files is attached as Exhibit 2. I also received five additional graphic files via email from the FTC. These were 44665.gif, 44666.gif, 45140.gif, 48873.gif and 54169.gif. My examination of these 194 graphic files used two different methods. My first method was to open the graphic in an image viewer and determine its characteristics and that it was viewable. The second method was to open the file in a hexeditor to verify the structure of the file. A hexeditor is a program designed to allow the editing of binary computer files.

As an example of these steps, I examined the file 44665.gif. The image below is the file opened in a graphic viewer.



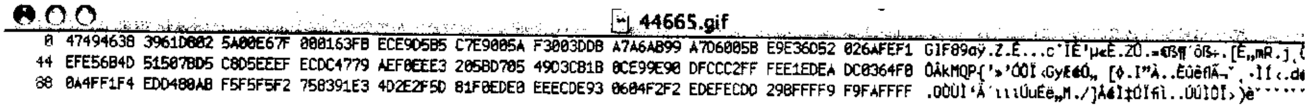
Your computer may be infected with spyware

This file has the following characteristics such as width and height.



Color Model	RGB
Depth	8
DPI Height	72
DPI Width	72
Has Alpha	1
Is Indexed	1
Pixel Height	90
Pixel Width	728

I then opened the file in a hexeditor and saw that the header corresponds to the GIF format. It begins with the tag GIF89a and the next four bytes match to the width and height of the graphic.

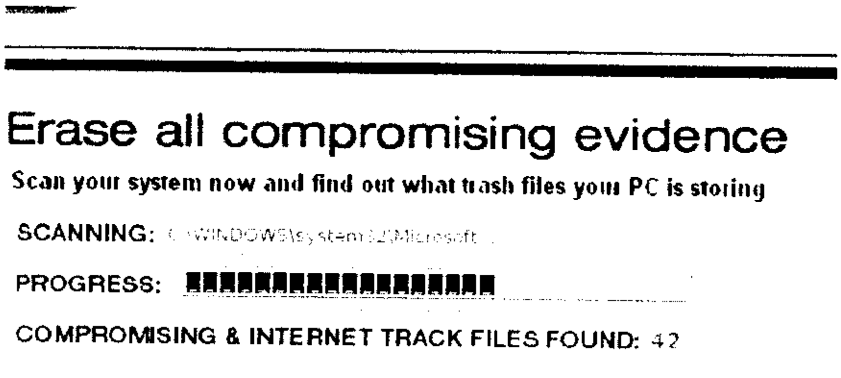


```
 0 47494638 3961D002 5A00E67F 000163FB ECE9D5B5 C7E9005A F3003DDB A7A6AB99 A706005B E9E36D52 026AFEF1 GIF89aÿ.Z.Ê...c˙ÌÊ'µ«Ê.ZÛ.=€ß¶´ôß÷.[Ê„mR.j,
44 EFE56B4D 51507BD5 C8D5EEEF ECDC4779 AEF0EEE3 205BD705 49D3CB1B 0CE99E90 DFCCC2FF FEE1EDEA DC0364F0 ÔÂkMQP{'»'ÕÔÎ‹Gy®ÓÓ„ [◊.I"À..ÊûêflÃ¬˘ .·Ìf‹.d
88 0A4FF1F4 EDD480AB F5F5F5F2 758391E3 4D2E2F5D 81F0EDE0 EEECDE93 0604F2F2 EDEFECDD 298FFFF9 F9FAFFFF .OÒÙÌ‘Ä´ıııÚuÉë„M./]Å‡ÌÏÌfiÌ..ÚÛÌÔÎ›)è˘˘˘˘
```

My examination of these graphic files found no sign that the files were anything more then graphics. As such, they have no way to detect malware on the client machine because they are graphic files and not executable.

The next step was to analyze the 20 Flash objects (SWF) included in exhibit 2 as well as BANNER_driveCleaner-dc-en.swf from the CD provided from the FTC. To analyze these files, I decompiled the SWF files and analyzed the resulting ActionScript code. ActionScript is the programming language used within SWF files that the developer/designer of the SWF file uses to have it perform various actions.

As an example of these steps, I examined the BANNER_driveCleaner-dc-en.swf file. My first step, as with the graphic files, was to open the file in the Flash Player to ensure the file was functioning.



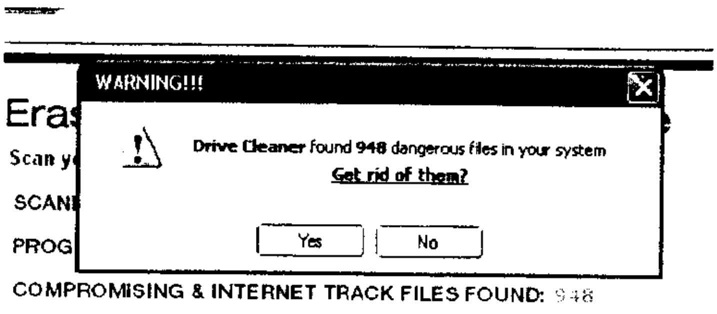
Erase all compromising evidence

Scan your system now and find out what trash files you PC is storing

SCANNING: C:\WINDOWS\system32\Microsoft

PROGRESS: ████████████████████

COMPROMISING & INTERNET TRACK FILES FOUND: 42



WARNING!!!

Drive Cleaner found 948 dangerous files in your system

Get rid of them?

COMPROMISING & INTERNET TRACK FILES FOUND: 948

As is shown in the screenshot, the SWF file purports to have found 948 "dangerous" Windows files. The SWF file displays a list of the Windows files scanned before displaying the message above. This "discovery" would be impossible for two reasons. First, the machine viewing the SWF file is a Linux machine and as such does not have any Windows files the SWF file supposedly scanned. The second reason is that the SWF file is not capable of scanning the file system because it does not contain any code to enable that type of scanning.

I then ran the program Flare to decompile the SWF file. Decompiling a program converts it from the executable state back into its programming language. The result was the following code.

```
      movie 'BANNER_driveCleaner-dc-en.swf' {
      // flash 6, total frames: 62, frame rate: 12 fps, 482x198 px,
compressed

        movieClip 93  {
        }

        button 95 {

          on (release) {
            getURL(CLICK_URL, '_self');
          }
        }

        frame 62 {
          stop();
        }
      }
```

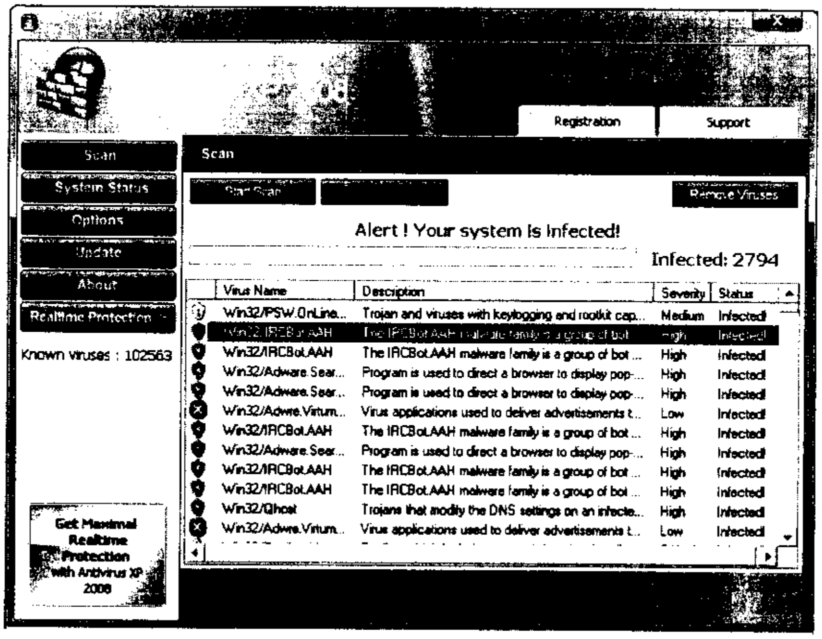
As is shown in the getURL line, this program opens a specific URL when the user clicks the ad. The HTML file loading the SWF provides this URL. The zip file that contained BANNER_driveCleaner-dc-en.swf also contained two JavaScript files, product.js and check.js. These files contained code to set browser cookies from drivecleaner.com and redirect the users to this domain. Each of other 20 SWF files analyzed contained links to freepcsecure.com and freerepair.org.

My analysis of these SWF files revealed that the only action taken by the ActionScript was to redirect a user to a web site. There was no code that accessed or scanned the file system. As with the graphic files, the look and feel of the vast majority of the SWF displays were made to imitate alerts and warnings. These files did not perform any scanning of the client system. Three of these files advertised work/shop at home information. These were MyS-728x90.swf, shopathome.swf and ua-answers.com-kuka-728x90.swf.

The final step of my analysis was to actually run the Windows binaries. To perform this test I created a Windows XP virtual machine that was not connected to the Internet and had only the default software installed with service pack 2 of Windows XP. This was done to ensure that the system was not infected with malware of any type. I used a virtual machine because it allowed me to create a snapshot of the pristine machine before running each piece of software. This virtual machine was running on a pristine Linux computer, which had also never been connected to the Internet.

I received a hard drive from the FTC that contained drive images that included the software I was asked to analyze. I mounted those images in a read-only mode and copied the software into the virtual machine, one piece of software at a time. The six pieces of software were WinAntiVirus2005ProScannerSetup, ErrorPatrolFreeSetup, PerformanceOptimizerFreeSetup, AntiMalwareGuard_Free, ErrorClean and AntivirusXP2008Installer.

To analyze each of the tools, I simply launched the executable. This then ran the program, which launched the purported scan of the system. All of the programs displayed a scan progress that included listing what file or process the scanner was examining. This display also included the list of alerts the program was alerting the user too. These alerts included items such as registry keys, system files and other items of supposed malware or privacy concern. The screenshot below shows one of these programs in action. It is AntivirusXP2008Installer.exe.



Scan

Alert ! Your system Is Infected!

Infected: 2794

Known viruses : 102563

Virus Name	Description	Severity	Status
Win32/PSW.OnLine...	Trojan and viruses with keylogging and rootkit cap...	Medium	Infected!
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot	High	Infected!
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Infected!
Win32/Adware.Sear...	Program is used to direct a browser to display pop-...	High	Infected!
Win32/Adware.Sear...	Program is used to direct a browser to display pop-...	High	Infected!
Win32/Adwre.Virtum...	Virus applications used to deliver advertisements t...	Low	Infected!
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Infected!
Win32/Adware.Sear...	Program is used to direct a browser to display pop-...	High	Infected!
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Infected!
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High	Infected!
Win32/Qhost	Trojans that modify the DNS settings on an infecte...	High	Infected!
Win32/Adwre.Virtum...	Virus applications used to deliver advertisements t...	Low	Infected!

The chart below outlines the number of alerts each software package "discovered" on the pristine XP machine.

Software Name	Alerts Reported
AntiVirusXP2008Installer	2,794 alerts
ErrorClean	96 alerts
AntiMalwareGuard_Free	27 alerts
PerformanceOptimizerFreeSetup	58 alerts
ErrorPatrolFreeSetup	308 alerts
WinAntiVirus2005ProScannerSetup	0 alerts

Conclusions

Based on my experience, the files I examined did nothing beyond displaying alerts to frighten users into paying for software. The graphic files were simply GIF format images that did nothing other then look like warning dialogs. Based on my experience, the Flash objects were also only displaying alert dialogs without the ability to actually scan the system. The executables are designed to appear to alert the user to malicious files, but actually report normal system files and nonexistent files as malicious. For example, these "scanners" reported cmd.exe, a standard Windows system file, as malicious. They also reported that the browser had evidence of having visited "adult-oriented" web sites even though this machine had never been connected to the Internet. In my opinion, these executables are only designed to scare the user the same as the other two types of files examined.

Feb 22, 2010

Kevin Johnson

Date

Exhibit 1

Kevin Johnson

2255 Elderberry Ct Orange Park, FL 32073 904-407-8024 kevin@inguardians.com

PROFESSIONAL EXPERIENCE

Senior Security Analyst

InGuardians *5/07 – Present*

As a Senior Security Consultant, I work with a large variety of corporate and government entities regarding their security posture. This ranges from network and application penetration testing to architecture reviews and custom training.

- Security Architecture Review
  - Application design, deployment and configuration review
  - Policy and procedure review
  - Network architecture and improvement review
- Penetration Testing and Vulnerability Assessment
  - Network-level penetration testing
  - Web application penetration testing
  - Vulnerability assessment
- Training in:
  - Operating System and Server Application Security
  - Intrusion Detection for System Administrators
  - Wireless Security
  - Development Security Methodologies

Certified Instructor

SANS *1/06 – Present*

Starting as a mentor for the Incident Handling and Hacker Techniques class, I have progressed to both the Stay Sharp program and the Community SANS as an instructor.

- Author and Primary Instructor for Security 542 Web Application Pen-Testing and Ethical Hacking
- Mentored 504 Incident Handling and Hacker Techniques
- Taught Computer and Network Security Awareness
- Taught Mastering Packet Analysis
- Taught Defeating Rogue Access Points
- Taught Google Hacking and Defense
- Taught IP Packet Analysis
- Taught 504 Incident Handling and Hacker Techniques
- Taught 504 Incident Handling and Hacker Techniques Bootcamp

Technical Architect II

BCBSF *8/05 – 5/07*

As the Linux architect for Service Delivery, I design, implement and manage the Linux infrastructure. I am also the architect for the Intel Server Security Response team. We are responsible for audits, baselines and security testing and monitoring.

- Linux integration within an enterprise environment
- Responsible for compliance auditing and testing
- Implemented various security tools including Nessus and Snort.
- Lead technician performing penetration tests

- Member of the Computer Incident Response Team

Technical Architect II

BCBSF *10/03 – 8/05*

As the Availability architect for Service Delivery, I work with teams during severity 1 problems to identify, troubleshoot and resolve the issue. I also work with the project management team to design, plan and implement projects.

- Lead SWAT team efforts to resolve production issues.
- Lead technician performing penetration tests
- Member of the Computer Incident Response Team
- Member of the Security Domain team
- Instructor for the EWTA Security Architecture class

System Administrator II

BCBSF / ACT, Jacksonville, FL *07/01 – 10/03*

As a WebSphere Administrator, I am responsible for maintaining the level 3 and level 4 web sites at Blue Cross/Blue Shield of Florida.

- Tested the security of the applications and the application servers
- Maintained the WebSphere Servers
- Maintained the HTTP servers
- Worked with the network team to implement changes needed by the various applications
- Perform upgrades and system maintenance
- Assist in architecting the applications
- Troubleshooting of applications and environments
- Member of the Computer Incident Response Team
- Member of the Security Domain team
- Instructor for the EWTA Security Architecture class

Senior Programmer Analyst III

ANC Rental Corporation, Ft. Lauderdale, FL *12/00 – 07/01*

ANC has the largest market share in the car rental industry. As a project lead, I managed and designed projects assigned to the IT department.

- Senior programmer on the QuickRent (Dexter) project for the Alamo.com web site.
- Project Lead for the LinkShare Affiliate program for Alamo.com
- Installed, configured and administrated the WebSphere server running Linux for the Warranty project.
- Lead developer for the component system used by the Membership project.
- Assisted as an administrator in the switch from Windows NT to an AIX/Linux based system.
- Assisted with the switch from VB components and ASP to Java and JSP
- Created a mentoring / code review system.
- Organized and taught UNIX and Java classes.
- Worked with the network infrastructure teams to implement and troubleshoot changes

Director of Software Development

Orlando.com / eSiteCreation, Coral Springs, FL *3/00 – 11/00*

Orlando.com, which then spun their development staff off as eSiteCreation, designed web sites in the travel arena. In this capacity, I served as head programmer and administrator in dealing with some of the biggest names in the travel industry, such as Sabre, Expedia and Travelocity.

Network Administrator / Web Application Developer

E-Z Legal Software, Deerfield Beach, FL 3/99 – 3/00

E-Z Legal Software is one of the largest suppliers of legal software and documents in the U.S. I was the head network administrator and lead the project to switch environments from Windows NT to Unix / Linux. I also performed various software development projects.

Y2K Consultant

American Express / TekSystems, Plantation, FL 8/98 – 3/99

American Express is one of the premier credit card companies. I was the project lead in the upgrade process to insure Y2K compliant systems.

Partner / Founder

Computer Data Interchange, Delray Beach, FL 4/92 – 8/98

Computer Data Interchange was a system integration company. My responsibilities included software development, project management, conducting the seminars. I was also responsible for managing the partner programs, working with investors, as well as daily operations.

VOLUNTEER EXPERIENCE

Project Lead / Founder

Basic Analysis and Security Engine (BASE) project

The BASE project is an analysis engine font-end to the Snort intrusion detection system. (IDS) With over 100,000 downloads from the SF.net site alone, BASE is the de facto standard web analysis tool for the Snort intrusion detection system. It is in use in places as diverse as the DoD to Cracker Barrel Restaurants. It has been translated into 18 languages and is used around the world.

Project Lead / Founder

Samurai Web Testing Framework LiveCD project

SamuraiWTF is a live environment focused on providing web penetration testing tools. It has been downloaded and used by thousands of penetration testers around the world. The project currently has seven volunteers that Kevin helps guide through the release cycle of a full Linux distribution.

Project Lead / Founder

Security Tools (SecTools) Project

SecTools is a collection of security tools that have been released with in the same project. Currently it is made up of the Windows version of Hping2, a packet generation utility. Nikto-NSE, a tool to generate NSE scripts for nmap. The Tweety project, which is a canary host system against malware and WebArmor, which will generate mod_security configurations to provide application level firewalls.

Speaker

Presentations at various institutions including: The SANS Institute, University of Florida, University of North Florida, Infragard, ISACA, ISSA, EPLUG, Jacksonville IT Council, DEFCON and ShmooCon

CERTIFICATIONS: GCIA, GCIH, GCFA, CISSP, GSPA, CEH, I-Net+, Certified System Expert IBM

Exhibit 2

Creative	Impressions
ag-15-bn-728x90-en.gif	84,651,488
468x60-warning-v1-f-s-en.gif	79,349,228
ag-15-bn-468x60-en.gif	70,909,768
728x90-adult-v1-a-f-s-en.gif	49,228,723
728x90-adult-v4-a-fred-s-en.gif	42,968,502
ag-er-bn1-468x60-en.gif	38,297,034
728x90-allin1-v1-en.gif	31,530,325
728x90-warning-v2-s-en.gif	28,180,766
728x90-warning-v1-f-s-en.gif	25,430,682
468x60-adult-v1-a-f-s-en.gif	25,375,383
ag-er-bnr-468x60-en.gif	24,629,206
728x90-warning-2buttons-v1-a-s-en.gif	21,822,337
468x60-systemerror-a-fhead-s-en.gif	21,249,175
728x90-warning-v2-f-s-en.gif	19,998,706
728x90-warning-redfixbutton-v1-a-s-en.gif	19,926,083
468x60-warning-v1-a-f-s-en.gif	19,575,592
468x60-adult-v1-a-fred-s-en.gif	18,713,709
468x60-warning-v1-a-fred-s-en.gif	17,362,149
728x90-warning-v1-a-f-s-br.gif	16,511,428
728x90-adult-2buttons-v1-a-s-en.gif	15,408,597
ag-fix-bn1-468x60-en.gif	15,056,941
120x600-scannow-v1-en.gif	14,420,160
120x600-warning-v3-s-en.gif	14,069,483
468x60-warning-2buttons-v1-a-s-en.gif	14,059,244
468x60-adult-v4-a-fred-s-en.gif	13,895,414
468x60-warning-2buttons-v2-a-s-en.gif	13,818,114
728x90-warning-2buttons-v2-a-s-br.gif	13,469,698
728x90-adult-2buttons-v3-a-s-en.gif	13,342,449
468x60-adult-v3-a-fred-s-en.gif	13,259,742
468x60-warning-redfixbutton2-a-s-en.gif	12,740,906
ag-sys-er-468x60_en.gif	12,201,413
ag-er-bnf-300x250-en.gif	11,598,394
120x600-scannow-v2-en.gif	10,399,657
aggr-er-bn-468x60-en.gif	9,779,172
ag-15-bn-120x600-en.gif	9,619,900
ag-er-bnf-728x90-en.gif	9,454,990
160x600-warning-v6-s-en.gif	7,717,388
ag-15-bn-728x90-es.gif	7,706,128
non-agg-dc-bn-468x60-en.gif	7,277,415
468x60-warning-2buttons-v3-a-s-en.gif	7,111,179
468x60-warning-redfixbutton1-a-s-en.gif	7,084,066
468x60-warning-bigfixbutton-a-s-en.gif	7,064,022
468x60-warning-v1-a-f-s-ja.gif	6,996,302

ag-15-bn-300x250-en.gif	6,613,250
advertiser.gif	6,611,987
ag-15-bn-468x60-nl.gif	6,458,915
ag-15-bn-468x60-fr.gif	6,345,886
468x60-warning-redfixbutton1-a-s-ja.gif	6,345,718
468x60-warning-v1-a-fred-s-ja.gif	6,292,349
120x600-warning-v7-s-en.gif	6,181,690
160x600-warning-v5-a-f-s-br.gif	6,143,735
120x600-adult-v1-a-f-s-en.gif	5,819,831
468x60-adult-v4-a-f-s-en.gif	5,780,351
468x60-warning-2buttons-v1-a-s-ja.gif	5,599,223
ag-15-bn-468x60-es.gif	5,386,496
120x600-adult-v4-a-fred-s-en.gif	5,358,677
468x60-adult-v2-a-f-s-en.gif	5,196,692
ag-er-bn1-468x60-nl.gif	5,163,494
468x60-warning-2buttons-v2-a-s-ja.gif	5,062,960
msn-freepcsecure1-728x90.swf	4,878,311
468x60-adult-2buttons-v3-a-s-en.gif	4,853,648
468x60-adult-v3-a-f-s-en.gif	4,818,673
468x60-adult-2buttons-v2-a-s-en.gif	4,805,709
160x600-allin1-v1-en.gif	4,796,563
160x600-warning-2buttons-v1-a-s-br.gif	4,639,781
ag-er-bnr-468x60-nl.gif	4,635,978
ag-er-bn1-468x60-es.gif	4,583,547
300x250-allin1-en.gif	4,434,510
ag-15-bn-160x600-en.gif	4,351,160
ag-15-bn-468x60-ja.gif	4,283,849
120x600-adult-2buttons-v1-a-s-en.gif	4,183,468
EN_468x60.gif	4,144,254
ag-er-bnr-468x60-es.gif	4,132,164
728x90-adult-content-v1-a-f-s-en.gif	4,128,279
728x90-warning-v2-f-s-es.gif	3,955,903
728x90-adult-v5-a-fred-s-en.gif	3,951,932
728x90-warning-redfixbutton-v1-a-s-es.gif	3,934,336
120x600-adult-2buttons-v3-a-s-en.gif	3,866,068
msn-freepcsecure-234x60g2.swf	3,859,685
728x90-adult-content-v2-a-f-s-en.gif	3,851,875
728x90-adult-v10-a-fred-s-en.gif	3,809,509
728x90-adult-v6-a-fred-s-en.gif	3,792,438
728x90-adult-v4-a-f-s-en.gif	3,787,192
ag-er-bnf-728x90-fr.gif	3,787,012
728x90-scannow-v1-en.gif	3,782,055
728x90-adult-v7-a-f-s-en.gif	3,780,733
728x90-adult-v9-a-fred-s-en.gif	3,759,283

728x90-warning-v1-f-s-es.gif	3,692,973
728x90-adult-content-v3-a-f-s-en.gif	3,670,829
160x600-wavp2007-download-v1-en.gif	3,576,947
160x600-wavp2007-download-v3-en.gif	3,537,457
728x90-adult-v8-a-fred-s-en.gif	3,511,942
468x60-warning-v1-f-s-ja.gif	3,510,948
728x90-adult-v9-a-fyellow-s-en.gif	3,475,176
160x600-wavp2007-download-v2-en.gif	3,469,563
300x250-adult-v4-a-fred-s-en.gif	3,446,238
ag-er-bn1-468x60-fr.gif	3,419,489
160x600-wavp-download-v3-en.gif	3,413,697
728x90-adult-family-v1-a-fred-s-en.gif	3,404,122
160x600-wavp-download-v2-en.gif	3,398,467
160x600-wavp-download-v1-en.gif	3,380,095
468x60-drivecleaner-v1-en.gif	3,338,024
728x90-warning-v2-s-es.gif	3,208,223
ag-er-bnr-468x60-fr.gif	3,163,081
728x90-adult-family-v2-a-fred-s-en.gif	3,127,581
728x90-adult-v8-a-fyellow-s-en.gif	3,055,481
468x60-warning-v1-a-f-s-sv.gif	3,044,477
120x600-warning-v1-f-s-en.gif	3,041,277
ag-er-bn1-468x60-jp.gif	3,019,993
nagg-bn-468x60-en.gif	2,886,017
nag-dc-bn-300x250-en.gif	2,867,964
728x90-adult-kids-v2-a-fred-s-en.gif	2,836,852
468x60-warning-v1-a-fred-s-sv.gif	2,827,870
468x60-warning-redfixbutton1-a-s-da.gif	2,800,640
ag-er-bnf-728x90-nl.gif	2,767,964
ag-er-bnf-468x60-pt.gif	2,761,683
728x90-warning-redfixbutton-v1-a-s-sv.gif	2,714,917
msn-freepcsecure-728x90-gnida.swf	2,680,900
468x60-adult-v2-a-fred-s-en.gif	2,661,073
ag-er-bnf-728x90-pt.gif	2,649,232
728x90-adult-v2-a-f-s-fr.gif	2,635,240
ag-er-bnr-468x60-jp.gif	2,628,319
ag-fix-bn1-468x60-jp.gif	2,558,423
728x90-adult-kids-v1-a-fred-s-en.gif	2,549,493
468x60-warning-v7-a-f-s-fr.gif	2,527,999
468x60-warning-v1-a-f-s-fr.gif	2,527,767
468x60-warning-v7-a-fred-s-fr.gif	2,524,029
468x60-warning-v4-a-f-s-fr.gif	2,516,269
ag-er-bn1-468x60-pt.gif	2,461,826
ag-er-bnf-728x90-es.gif	2,441,751
468x60-warning-2buttons-v2-a-s-sv.gif	2,395,118

468x60-warning-v5-a-f-s-fr.gif	2,371,622
msn-freepcsecure1-300x250.swf	2,355,324
468x60-warning-v1-a-f-s-da.gif	2,348,777
nagg-bn-468x60-pt.gif	2,310,477
ag-fix-bn1-468x60-fr.gif	2,282,790
300x250-adult-v1-a-f-s-en.gif	2,264,587
468x60-warning-redfixbutton1-a-s-sv.gif	2,256,499
ag-er-bn1-468x60-sw.gif	2,214,952
468x60-warning-v1-f-s-fr.gif	2,191,262
ag-er-bnf-120x600-pt.gif	2,159,983
nag-dc-bn-728x90-en.gif	2,124,741
nagg-er-EN-468x60.gif	2,115,910
ag-er-bnf-728x90-ja.gif	2,082,973
ag-15-bn-468x60-sv.gif	1,994,399
ag-er-bn1-468x60-no.gif	1,991,545
ag-er-bnr-468x60-sw.gif	1,972,661
468x60-warning-v1-a-f-s-nl.gif	1,920,294
ag-er-bnr-468x60-no.gif	1,908,143
728x90-warning-v2-f-s-sv.gif	1,898,911
ag-fix-red-bn1-728x90-en.gif	1,877,343
nagg-er-bn-468x60-pt.gif	1,856,857
ag-er-bnf-728x90.se.gif	1,832,835
ag-15-bn-468x60-no.gif	1,780,686
468x60-warning-v1-a-fred-s-nl.gif	1,770,937
msn-freepcsecure-728x90g2.swf	1,763,357
msn-freerepair-728x90.swf	1,731,343
ag-fix-bn1-468x60-no.gif	1,721,419
300x250-warning-v1-f-s-en.gif	1,715,243
468x60-warning-v1-f-s-sv.gif	1,692,794
br_468.gif	1,669,510
468x60-warning-v1-a-fred-s-da.gif	1,641,105
468x60-systemerror-a-fhead-s-es.gif	1,608,088
shopathometv.swf	1,607,591
br_468-05op.gif	1,535,902
ag-er-bnr-468x60-pt.gif	1,531,160
468x60-warning-v1-a-f-s-es.gif	1,455,702
msn-freepcsecure-468x60g2.swf	1,449,660
300x250-warning-v1-f-s-pt.gif	1,385,959
ag-fix-red-bn1-468x60-nl.gif	1,355,839
468x60-warning-v1-a-fred-s-es.gif	1,336,685
ag-fix-bn-468x60-pt.gif	1,331,803
msn-freepcsecure-300x250-gnida.swf	1,279,725
728x90-adult-v2-a-f-s-de.gif	1,274,339
nagg-Protect-ad-120x600-en.gif	1,236,558

468x60-warning-2buttons-v2-a-s-es.gif	1,220,322
BR2_468x60_gif.gif	1,209,092
nagg-Protect-ad-160x600-en.gif	1,183,242
nagg-Protect-ad-728x90-en.gif	1,181,488
468x60-warning-2buttons-v1-a-s-es.gif	1,179,159
ag-fix-bn1-468x60-pt.gif	1,159,937
ag-fix-bn-468x60-en.gif	1,146,108
msn-freepcsecure-180x150.swf	1,121,563
BR1_468x60_gif.gif	1,116,977
300x250-warning-2buttons-s-pt.gif	1,109,083
wav-pro-en.gif	1,090,357
468x60-warning-v1-a-f-s-no.gif	1,066,654
nagg-Protect-ad-300x250-en.gif	1,065,399
msn-freepcsecure-160x600.swf	1,058,268
468x60-warning-v1-a-fred-s-no.gif	1,022,568
468x60-warning-redfixbutton1-a-s-es.gif	997,305
nag-dc-bn-160x600-en.gif	995,837
120x600-ebooks.gif	988,869
MyS-728x90-flash_.swf	939,696
ua-answers.com-kuka-728x90.swf	922,724
bn-dc-120x600-en.gif	918,924
msn-freepcsecure-180x150g2.swf	876,512
nag-dc-bn-120x600-en.gif	854,087
ag-er-bnf-300x250-pt.gif	842,763
ag-15-bn-468x60-pt.gif	833,808
msn-freepcsecure-180x150-gnida.swf	801,059
msn-freepcsecure1-468x60.swf	801,012
468x60-virus-v2-en.gif	717,061
msn-freerepair-300x250.swf	715,203
msn-freepcsecure-160x600-gnida.swf	629,500
728x90-casino-aceking.gif	578,008
msn-freepcsecure-300x250g2.swf	571,400
ag-er-bnf-1-468x60-pt.gif	551,149
msn-freerepair-160x600.swf	522,081
TOTAL	1,379,533,158

RDX 34

Expert Report of Kevin Johnson

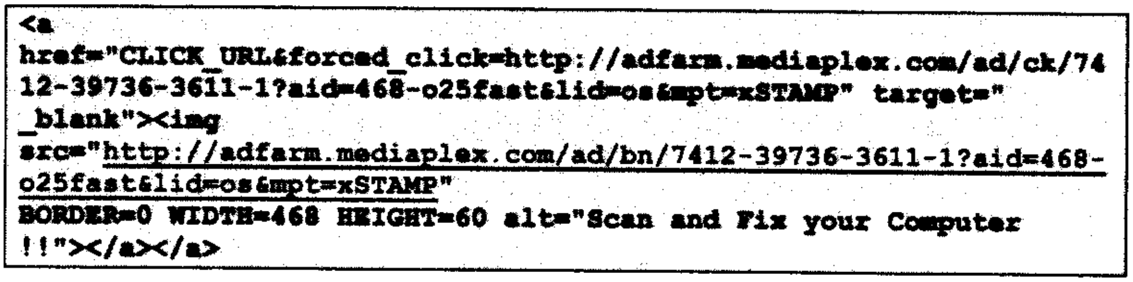
I. Introduction

In April of 2010, I was asked by the Federal Trade Commission to review three expert reports that were submitted in response to my report. These reports purported to respond to my findings, but as I will outline through this report, there were a number of mistakes and unrelated items. Overall, the reports I reviewed in no way refuted what I found and in the most part, I find them irrelevant to my initial report. In each of the reports there were numerous issues in addressing my main finding; which is that the main purpose of these files were to sell software through false reports and fake scan alerts. The two reports from Daniel Kim and Scott Ellis are addressed below; the report from James Langenfeld does not address my report except to say that he knows of Daniel Kim's results.

II. Response to the Kim and Ellis Reports

There are two main pieces of my original analysis that the Kim and Ellis reports disagreed with. The first was the flash objects and graphic files. In my analysis, these files were found to not be able to scan the system viewing them. Daniel Kim acknowledges that the graphic files are not capable of scanning the system in his report.

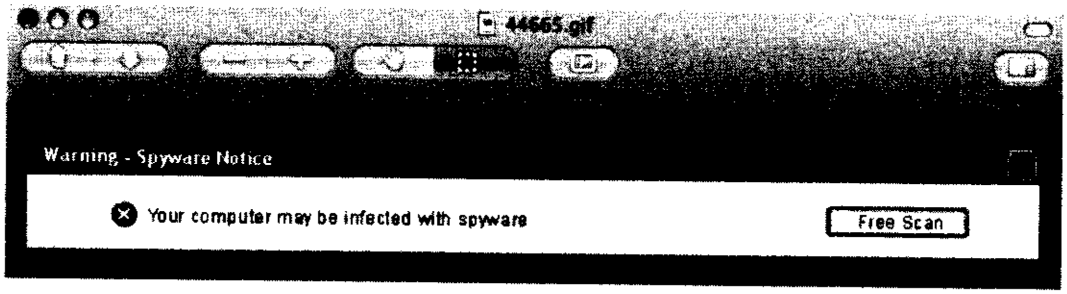
Yet, in both the Kim and Ellis reports, they attempt to say that this finding was not conclusive since I did not analyze the "wrapper" code that loaded the graphics. While I believe this statement to be flawed, I did request a copy of the code used by the ad display network. It is necessary to point out that ad display networks typically accepted graphic files and flash objects and the network handles providing the HTML code necessary to display the ad. An example of the code snippets I received in the Mediaplex report titled *Summary of Investigation Carried out by Mediaplex on Revenue Response Activity* is below.



```
<a
href="CLICK_URL&forced_click=http://adfarm.mediaplex.com/ad/ck/74
12-39736-3611-1?aid=468-o25fast&lid=os&mpt=xSTAMP" target="
_blank"><img
src="http://adfarm.mediaplex.com/ad/bn/7412-39736-3611-1?aid=468-
o25fast&lid=os&mpt=xSTAMP"
BORDER=0 WIDTH=468 HEIGHT=60 alt="Scan and Fix your Computer
!!"></a></a>
```

This code was used to display the item *CID 55182*. As we can see in this example, the HTML code is a simple anchor tag (<a href>) that contains an image tag (<img>). What this does is load the graphic file from the *adfarm.mediaplex.com* server. If a person viewing this ad clicks on the image, their browser will browse to the address within the *href* attribute of the anchor tag. In this example, we see none of the supposed "wrapper" scanning code that Mr. Kim and Mr. Ellis said might exist.

Furthermore, Mr. Ellis' report discusses that by not analyzing the entire HTML site, I missed crucial pieces of information that would let the user know that the scan was not a real scan. My report and expert opinion is that ads such as the examples below are designed to appear as pop-up warnings.



Warning - Spyware Notice

Your computer may be infected with spyware

The above graphic is the gif file 44665.gif. As is visible, it appears to be a Windows warning dialog.

Mr. Kim's report also goes on to state that I need to analyze the "server side" code to determine if that code performed any scanning. I find this to be irrelevant to my report as the HTML code that I examined above did not load any server-side code or reference it before loading the graphics that purported to warn the users of malicious content on their systems.

It is important to note that the defendants' ads were displayed around the Internet on various web sites. These sites were built and managed by other people and as such, the defendants had no ability to add content to these sites outside of the content the ad display network has provided.

The second main point within the responses to my report was directed at the analysis of the windows binaries. Both the Kim and Ellis reports included analysis of various pieces of scanning software. The first interesting note is that out of the six pieces of software Daniel Kim and the eight that Scott Ellis analyzed, only three matched with the software in my report. I assume this means that they agree with the rest of my findings regarding the remaining software. These three overlapping files were ErrorPatrolFreeSetup, WinAntivirus2005ProScannerSetup and PerformanceoptimizerFreeSetup. The md5 hashes of the files I analyzed are below:

ErrorPatrolFreeSetup.exe	da9fe65859ac9651aede8fdc47f5ce4b
PerformanceoptimizerFreeSetup.exe	a988ad089e7b11887585df0bee963863
WinAntiVirus2005ProScannerSetup.exe	09a687d47bd96538d3333a5263751853

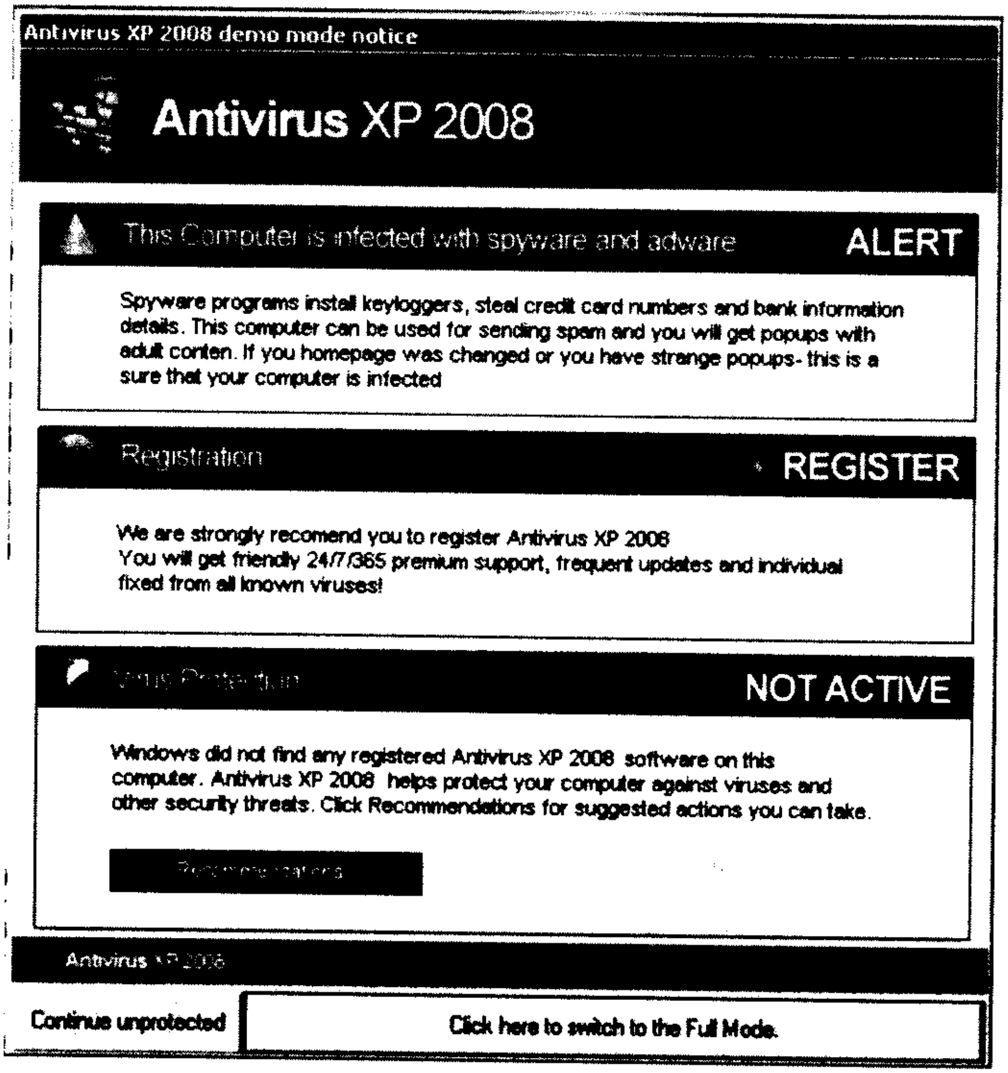
It appears that the majority of the Ellis and Kim reports are analyzing the paid versions of the software. I think its important to note that the process of using the free version compared to the paid version is quite different to the end user. In my experience, the paid version of the software I tested forces the user go through a activation verification before each use and the software tones down the extreme alerts and extreme warning language used to explain findings to the user. The free versions, on the other hand, have no activation process and use false and scary language to lure users into purchasing the paid version. This is done through buttons for registration or pop-ups when the user tries to access a function that requires payment.

Daniel Kim's report analyzed six different scanning software packages. All six of the versions he listed as tested were the paid versions of the applications. We can tell this by the simple fact that the tools offered the ability to take action on the system after they prompted me for my registration details when I ran them. Other then System Doctor, they also thanked me for either purchasing or registering them. While the purchased versions of the software may be interesting to Mr. Kim, they have no relevance to my report, which focuses on the free versions of the scanning software, it concludes that they alerted on either non-malicious items or outright false ones in order to convince consumers to purchase the product.

During my verifying that Mr. Kim tested the paid versions of the software I did notice two interesting points. The first is that none of the paid versions used the extreme warning dialogs and extremist language seen in the free versions. My expert opinion is that this is because they have already sold the software, which was the goal of that language. The second item of interest is that the software Mr. Kim lists as analyzed, WinAntiVirus2005ProSetup, does not match the screenshots on page 11 of his report. They include text in the title bar regarding "Spyware, Viurses (sic), and Hackers" as well as a "Register Now" button. The software he listed does not include either of those.

Mr. Ellis' report analyzes eight different pieces of software, three of which were in my report. The majority of this section of his report focuses on running the paid versions of the software and then stating without much discussion that the free versions are similar. Again, this does not address my report's finding that I found alarmist and misleading alerts in the free software I analyzed.

The screenshot below is an example of invalid alerts designed to scare a user into purchasing the scanning software.


Antivirus XP 2008 demo mode notice
Antivirus XP 2008
This Computer is infected with spyware and adware
ALERT
Registration
REGISTER
Virus Protection
NOT ACTIVE
Recommendations
Antivirus XP 2008
Continue unprotected
Click here to switch to the Full Mode.

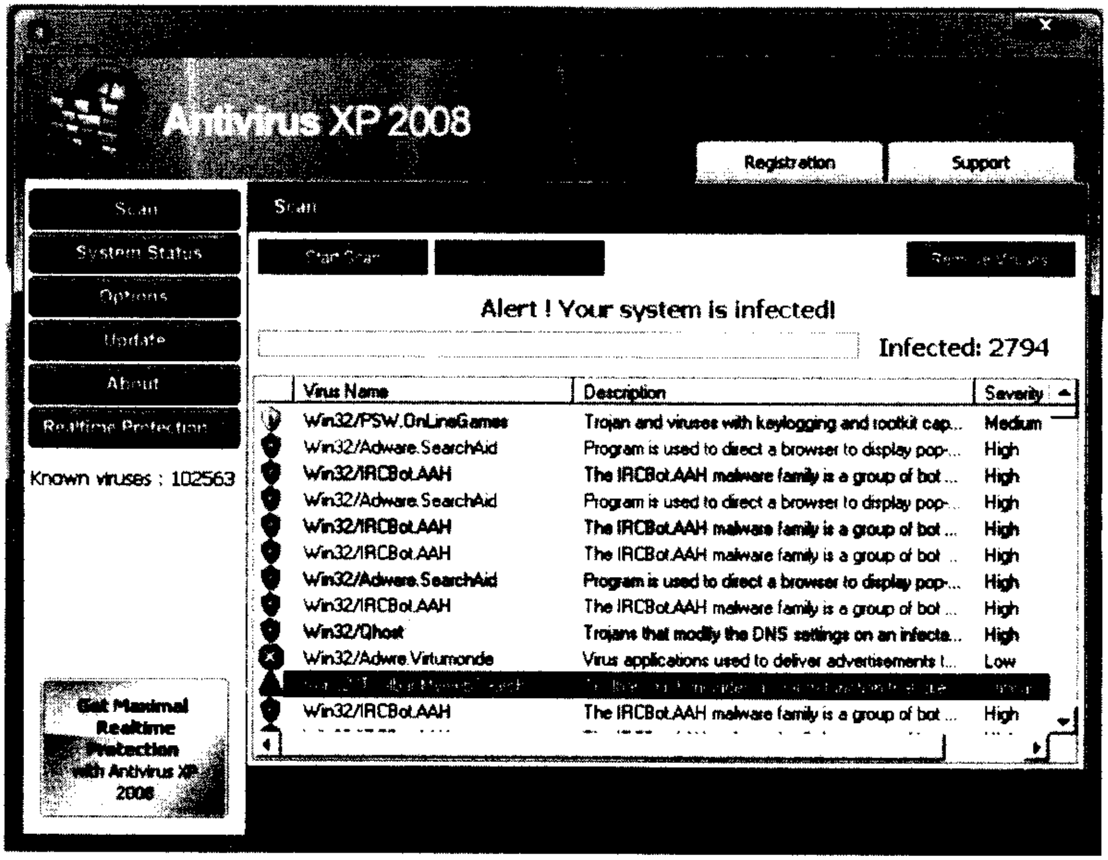
Spyware programs install keyloggers, steal credit card numbers and bank information details. This computer can be used for sending spam and you will get popups with adult conten. If you homepage was changed or you have strange popups- this is a sure that your computer is infected

We are strongly recomend you to register Antivirus XP 2008
You will get friendly 24/7/365 premium support, frequent updates and individual fixed from all known viruses!

Windows did not find any registered Antivirus XP 2008 software on this computer. Antivirus XP 2008 helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take.

This package, AntiVirusXP2008Installer (md5 hash: be4d8f09249a32d5b93163e3c1133e92) alerts on 2,794 items on the system. In the screenshot we see alerts reporting that the system is infected with malware such as the MyWebSearch Toolbar and various bots. These alerts are rated as critical and high levels of threat. Since this was run on a fresh install of Windows XP SP2 that was never connected to the Internet, these alerts cannot be accurate. As such they are designed to scare the user.

We also see in the next screenshot where the software purports to have found a "CyberTerrorist virus", which supposedly uses your computer to attack government machines. It is humorous to note that the software finds this to be only a medium risk to the user. This alert is repeated a large number of times throughout the interface.



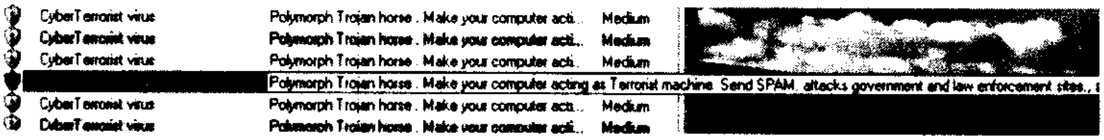
Known viruses : 102563

Alert ! Your system is infected!

Infected: 2794

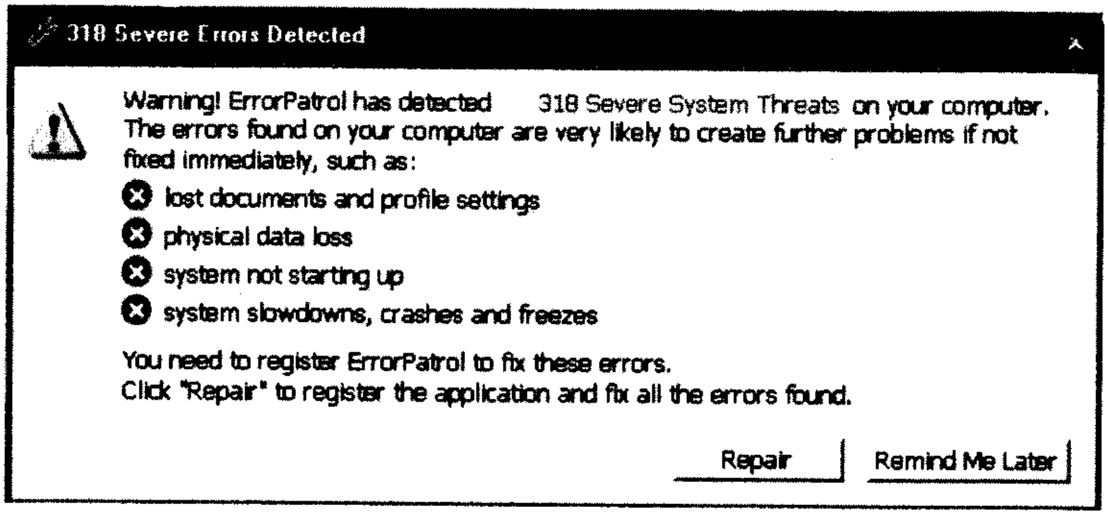
Virus Name	Description	Severity
Win32/PSW.OnLineGames	Trojan and viruses with keylogging and rootkit cap...	Medium
Win32/Adware.SearchAid	Program is used to direct a browser to display pop-...	High
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High
Win32/Adware.SearchAid	Program is used to direct a browser to display pop-...	High
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High
Win32/Adware.SearchAid	Program is used to direct a browser to display pop-...	High
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High
Win32/Qhost	Trojans that modify the DNS settings on an infecte...	High
Win32/Adwre.Virtumonde	Virus applications used to deliver advertisements t...	Low
[illegible]	[illegible]	[illegible]
Win32/IRCBot.AAH	The IRCBot.AAH malware family is a group of bot ...	High

The below screenshot is the tooltip description of the Cyberterrorist virus.



CyberTerrorist virus	Polymorph Trojan horse . Make your computer acti...	Medium
CyberTerrorist virus	Polymorph Trojan horse . Make your computer acti...	Medium
CyberTerrorist virus	Polymorph Trojan horse . Make your computer acti...	Medium
	Polymorph Trojan horse . Make your computer acting as Terrorist machine. Send SPAM, attacks government and law enforcement sites.,	
CyberTerrorist virus	Polymorph Trojan horse . Make your computer acti...	Medium
CyberTerrorist virus	Polymorph Trojan horse . Make your computer acti...	Medium

Next, lets look at the alerts from ErrorPatrolFreeSetup (md5 hash: da9fe65859ac9651aede8fdc47f5ce4b). ErrorPatrolFreeSetup also scans the system to find errors and misconfigurations on the client machines. While as Mr. Ellis points out, there are a number of tools that perform this type of scan, I believe that the wording and presentation of the ErrorPatrol alerts is misleading.



318 Severe Errors Detected

Warning! ErrorPatrol has detected 318 Severe System Threats on your computer. The errors found on your computer are very likely to create further problems if not fixed immediately, such as:

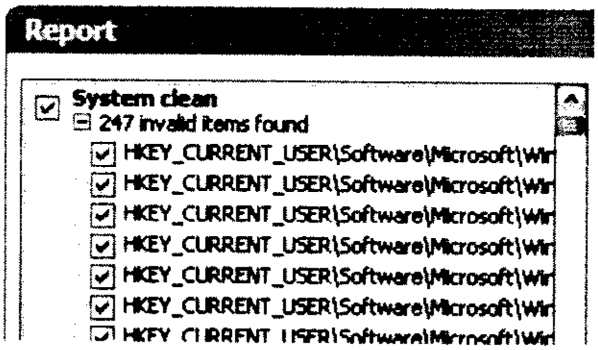
- lost documents and profile settings
- physical data loss
- system not starting up
- system slowdowns, crashes and freezes

You need to register ErrorPatrol to fix these errors.
Click "Repair" to register the application and fix all the errors found.

As we can see in the above screenshot, the ErrorPatrol software warns that the user's system contains *severe system threats* that cause fear-inducing items such as:

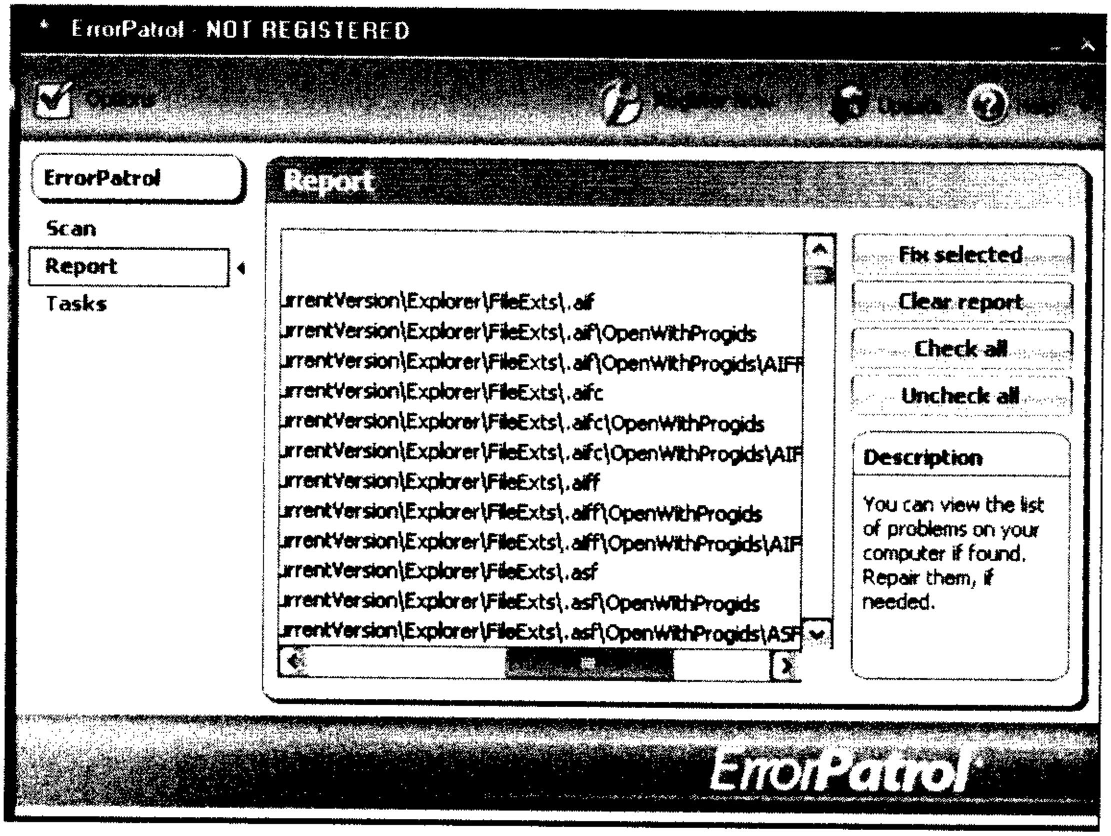
- Lost documents and profile settings
- Physical data loss
- The system not starting up
- System slowdowns, crashes and freezes

After closing this extreme warning message, I am able to see that the majority of the *findings* are simple registry keys that exist in every install of Windows. These registry keys are related to file handling and the registration of tools for specific file types.



Report

☑ System clean
⊟ 247 invalid items found
☑ HKEY_CURRENT_USER\Software\Microsoft\Wi
☑ HKEY_CURRENT_USER\Software\Microsoft\Wi
☑ HKEY_CURRENT_USER\Software\Microsoft\Wi
☑ HKEY_CURRENT_USER\Software\Microsoft\Wi
☑ HKEY_CURRENT_USER\Software\Microsoft\Wi
☑ HKEY_CURRENT_USER\Software\Microsoft\Wi
☑ HKEY_CURRENT_USER\Software\Microsoft\Wi



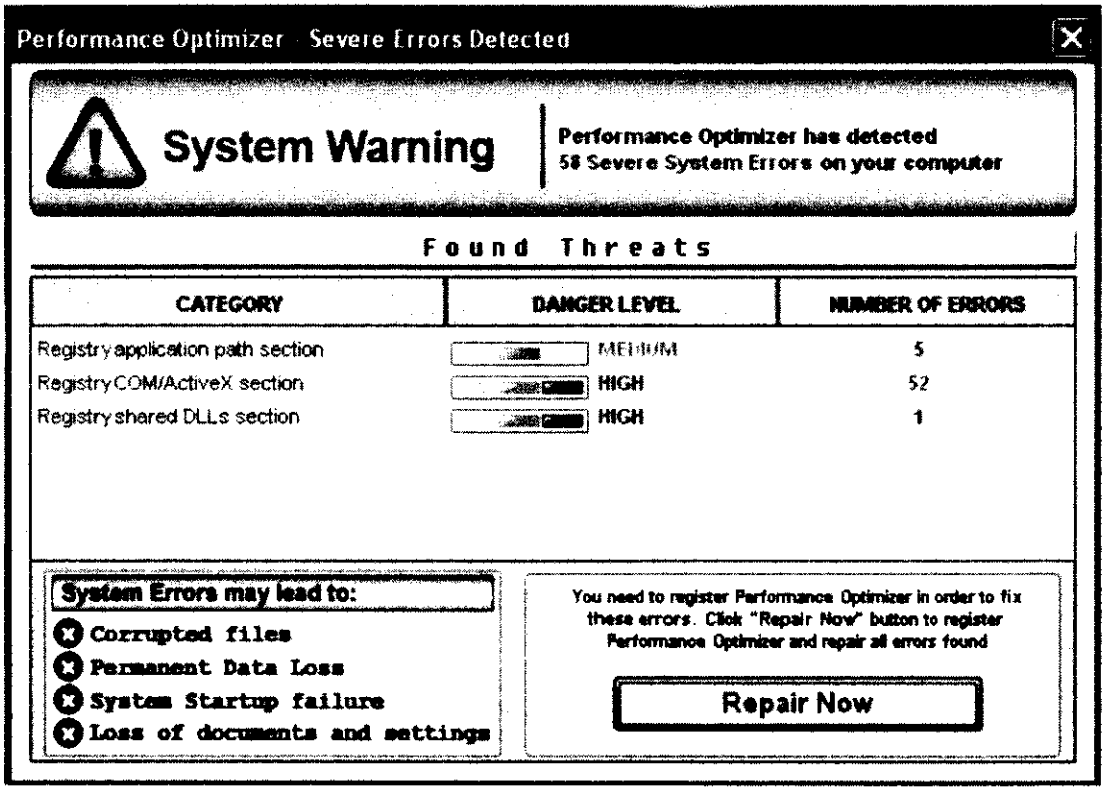
```
urrentVersion\Explorer\FileExts\.aif
urrentVersion\Explorer\FileExts\.aif\OpenWithProgids
urrentVersion\Explorer\FileExts\.aif\OpenWithProgids\AIFF
urrentVersion\Explorer\FileExts\.aifc
urrentVersion\Explorer\FileExts\.aifc\OpenWithProgids
urrentVersion\Explorer\FileExts\.aifc\OpenWithProgids\AIF
urrentVersion\Explorer\FileExts\.aiff
urrentVersion\Explorer\FileExts\.aiff\OpenWithProgids
urrentVersion\Explorer\FileExts\.aiff\OpenWithProgids\AIF
urrentVersion\Explorer\FileExts\.asf
urrentVersion\Explorer\FileExts\.asf\OpenWithProgids
urrentVersion\Explorer\FileExts\.asf\OpenWithProgids\ASF
```

Description

You can view the list of problems on your computer if found. Repair them, if needed.

These registry keys are used to choose which software package is used when a user double-clicks on a file with that extension. Since Windows does not contain software able to run these file types by default, the registry key is empty. This setting would not cause any of the types of problems listed in the warning message from ErrorPatrolFreeSetup. It would be impossible for these registry keys to cause any of the events warned about by this software.

I also ran PerformanceOptimizerFreeSetup (md5 hash: a988ad089e7b11887585df0bee963863) to capture the methods it used to alert the user. As with the other tools we can see in the below screenshot, that it uses alarmist language.



Performance Optimizer - Severe Errors Detected

System Warning

Performance Optimizer has detected
58 Severe System Errors on your computer

Found Threats

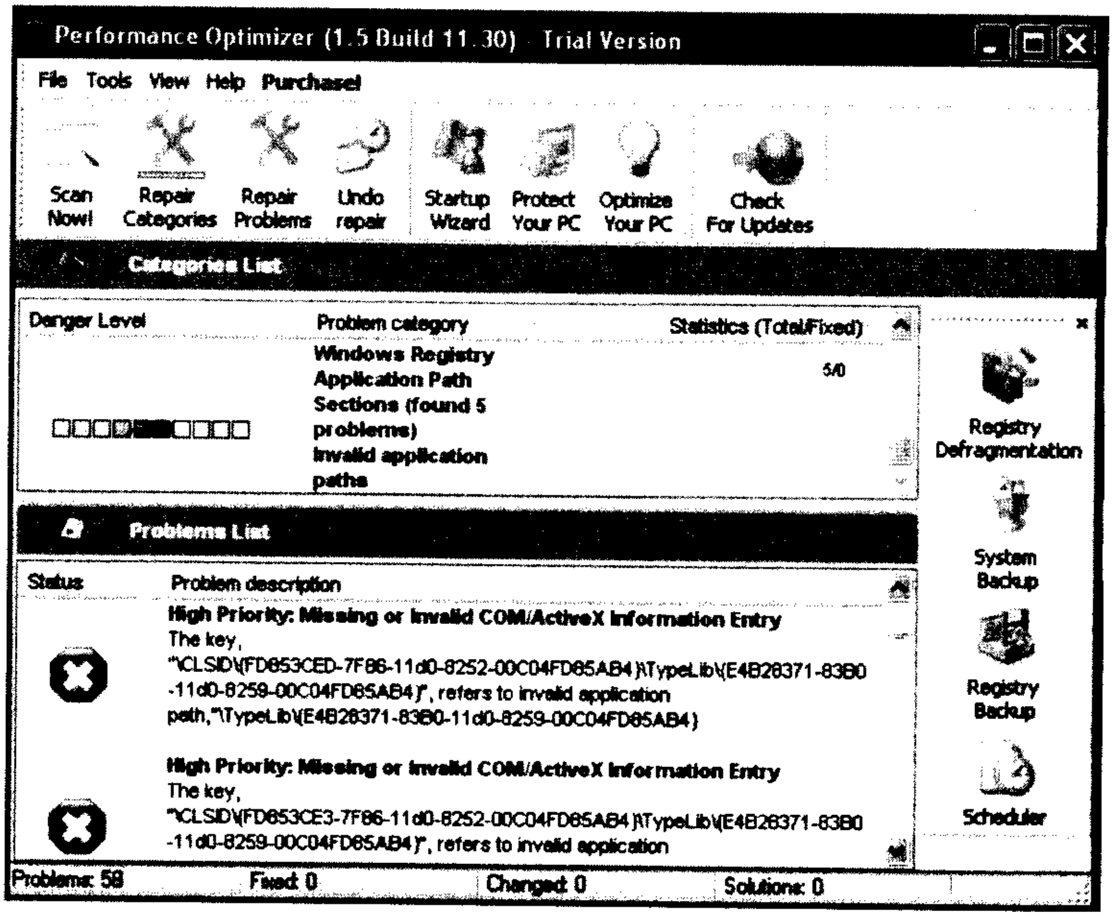
CATEGORY	DANGER LEVEL	NUMBER OF ERRORS
Registry application path section	MEDIUM	5
Registry COM/ActiveX section	HIGH	52
Registry shared DLLs section	HIGH	1

System Errors may lead to:

- Corrupted files
- Permanent Data Loss
- System Startup failure
- Loss of documents and settings

You need to register Performance Optimizer in order to fix these errors. Click "Repair Now" button to register Performance Optimizer and repair all errors found

The dialog warns that the "severe system errors" it has detected may cause corrupted files, permanent data loss and system startup failures. When I look at the results, I see the following:



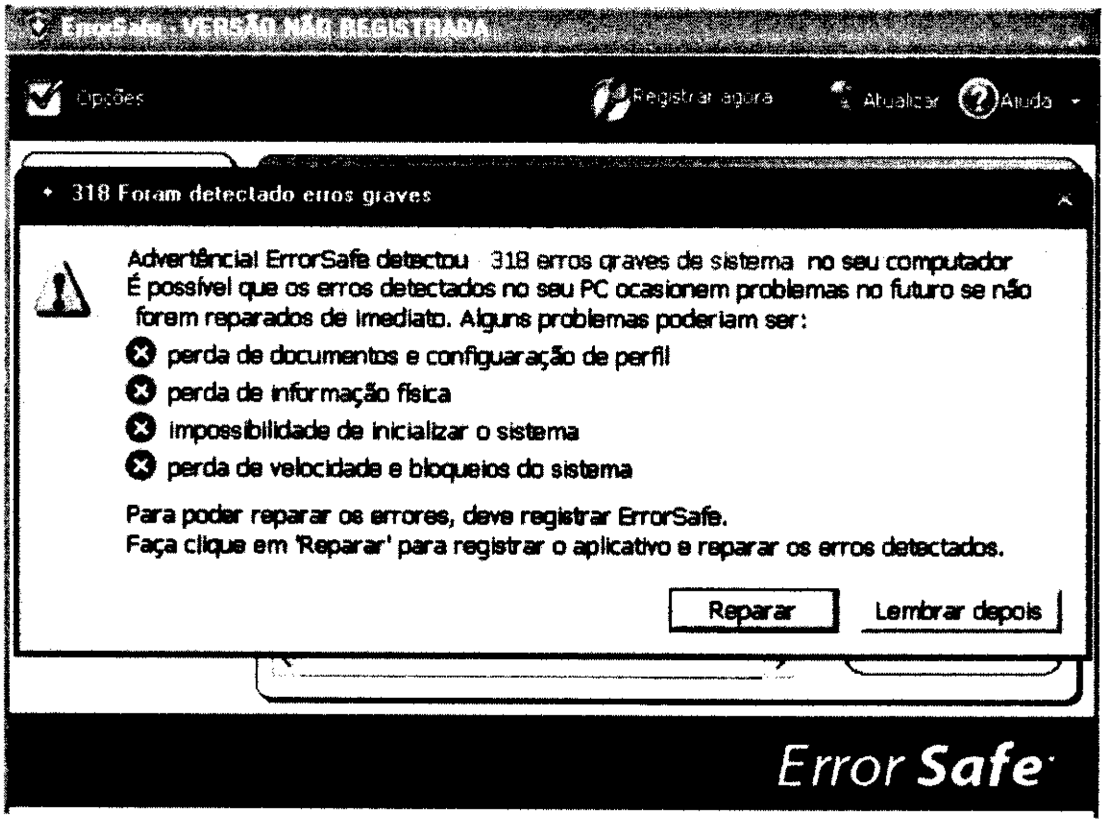
Danger Level	Problem category	Statistics (Total/Fixed)
□□□□▨■□□□□	Windows Registry Application Path Sections (found 5 problems) Invalid application paths	5/0

Status	Problem description
⊗	**High Priority: Missing or Invalid COM/ActiveX Information Entry** The key, "\CLSID\{FD853CED-7F86-11d0-8252-00C04FD85AB4}\TypeLib\{E4B28371-83B0-11d0-8259-00C04FD85AB4}", refers to invalid application path,"\TypeLib\{E4B28371-83B0-11d0-8259-00C04FD85AB4}
⊗	**High Priority: Missing or Invalid COM/ActiveX Information Entry** The key, "\CLSID\{FD853CE3-7F86-11d0-8252-00C04FD85AB4}\TypeLib\{E4B28371-83B0-11d0-8259-00C04FD85AB4}", refers to invalid application

Problems: 58 Fixed: 0 Changed: 0 Solutions: 0

These warning have no chance of causing the widespread havoc the warning message claims. Again, this language is used to scare the user into purchasing the full version of the software.

To further explore these software packages, I ran ErrorSafeFreeSetup_br (md5 hash: fe8f516782a9fcfb3fdfe5346ea3590d). I chose this software since Daniel Kim analyzed the paid version of ErrorSafe in his report and I wanted to test the free version. While I do not speak or read Portuguese, as we can see in the below screenshot, the warning message appears to be the same as the one from ErrorPatrolFreeSetup.



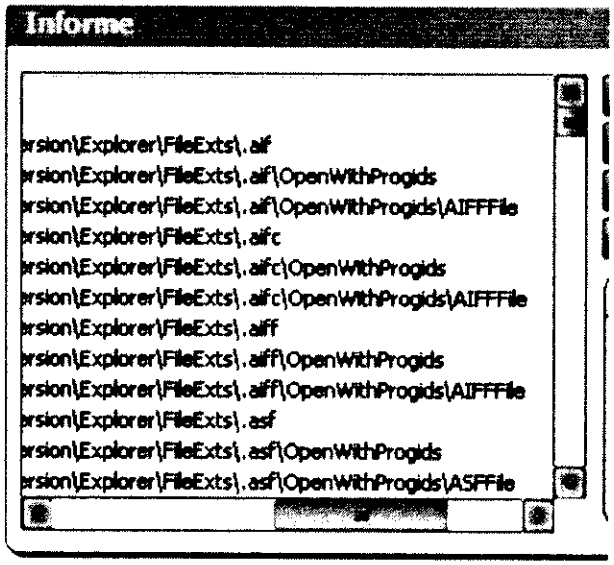
318 Foram detectado erros graves

Advertência! ErrorSafe detectou 318 erros graves de sistema no seu computador
É possível que os erros detectados no seu PC ocasionem problemas no futuro se não forem reparados de imediato. Alguns problemas poderiam ser:

- perda de documentos e configuaração de perfil
- perda de informação física
- impossibilidade de inicializar o sistema
- perda de velocidade e bloqueios do sistema

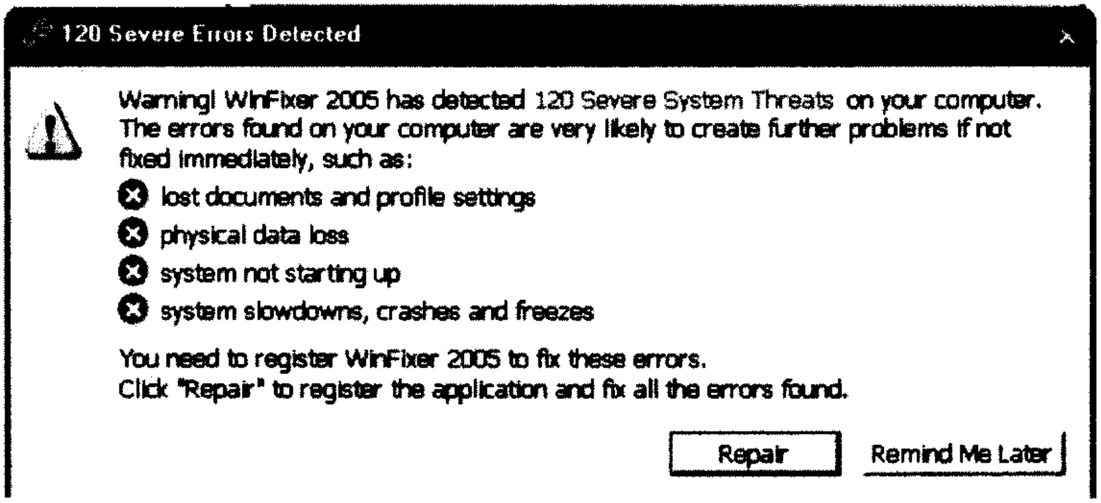
Para poder reparar os errores, deve registrar ErrorSafe.
Faça clique em 'Reparar' para registrar o aplicativo e reparar os erros detectados.

After we clear that message and examine the list of "*errors graves de sistema*", we see the same exact registry settings being reported.



```
rsion\Explorer\FileExts\.aif
rsion\Explorer\FileExts\.aif\OpenWithProgids
rsion\Explorer\FileExts\.aif\OpenWithProgids\AIFFFile
rsion\Explorer\FileExts\.aifc
rsion\Explorer\FileExts\.aifc\OpenWithProgids
rsion\Explorer\FileExts\.aifc\OpenWithProgids\AIFFFile
rsion\Explorer\FileExts\.aiff
rsion\Explorer\FileExts\.aiff\OpenWithProgids
rsion\Explorer\FileExts\.aiff\OpenWithProgids\AIFFFile
rsion\Explorer\FileExts\.asf
rsion\Explorer\FileExts\.asf\OpenWithProgids
rsion\Explorer\FileExts\.asf\OpenWithProgids\ASFFile
```

I also ran WinFixer2005ScannerSetup_jp (md5 hash: 720b7e2b2b607c2aaf38d96887dc9988) to match a free version to the paid version of WinFixer Kim ran. As with the other software, we received the following grave and false warning was shown.



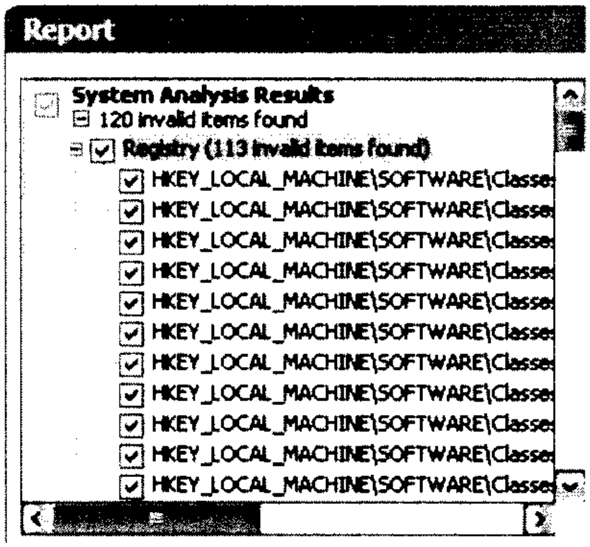
120 Severe Errors Detected

Warning! WinFixer 2005 has detected 120 Severe System Threats on your computer. The errors found on your computer are very likely to create further problems if not fixed immediately, such as:

- ☒ lost documents and profile settings
- ☒ physical data loss
- ☒ system not starting up
- ☒ system slowdowns, crashes and freezes

You need to register WinFixer 2005 to fix these errors.
Click "Repair" to register the application and fix all the errors found.

Again the software talks about "Severe System Threats", even highlighting it in red. It warns that catastrophic errors are "*very likely*" to be caused by the errors found. But as with the other pieces of software, when we look at the results, we find a different story.

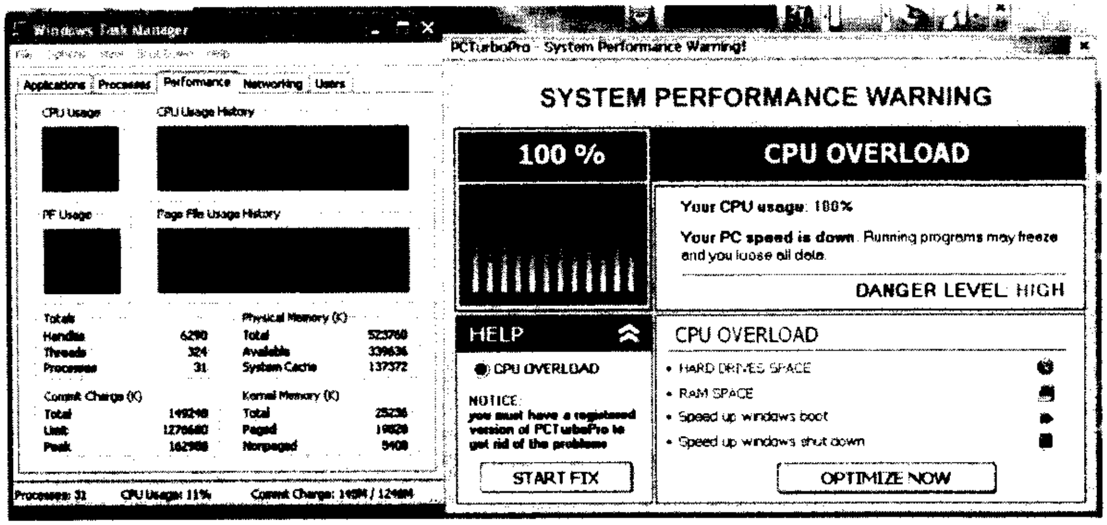


Report

System Analysis Results
⊟ 120 invalid items found
⊟ ☑ Registry (113 invalid items found)
☑ HKEY_LOCAL_MACHINE\SOFTWARE\Classe
☑ HKEY_LOCAL_MACHINE\SOFTWARE\Classe
☑ HKEY_LOCAL_MACHINE\SOFTWARE\Classe
☑ HKEY_LOCAL_MACHINE\SOFTWARE\Classe
☑ HKEY_LOCAL_MACHINE\SOFTWARE\Classe
☑ HKEY_LOCAL_MACHINE\SOFTWARE\Classe
☑ HKEY_LOCAL_MACHINE\SOFTWARE\Classe
☑ HKEY_LOCAL_MACHINE\SOFTWARE\Classe
☑ HKEY_LOCAL_MACHINE\SOFTWARE\Classe
☑ HKEY_LOCAL_MACHINE\SOFTWARE\Classe
☑ HKEY_LOCAL_MACHINE\SOFTWARE\Classe

Again, we find simple registry keys are missing values or are not set the way this software thinks is best. It is impossible these registry keys could cause the kinds of issues warned about in the warning dialog.

I also ran PCTurboProSetupFree (md5 hash: e46fb0129bbae5f741b43ea33e4b70e6) to see what type of behavior this package exhibits. This is yet another free version of the software viewed in comparison to the paid versions Kim and Ellis tested. When it launched, the software displayed a toolbar at the top of the screen that allowed the user to scan for system problems or performance issues with the machine. When I clicked the CPU button, l received the following warning message.



Windows Task Manager

Applications | Processes | Performance | Networking | Users

CPU Usage — CPU Usage History

PF Usage — Page File Usage History

Totals		Physical Memory (K)	
Handles	6290	Total	523768
Threads	324	Available	339636
Processes	31	System Cache	137372

Commit Charge (K)		Kernel Memory (K)	
Total	149240	Total	25236
Limit	1276680	Paged	19828
Peak	162988	Nonpaged	5408

Processes: 31 CPU Usage: 11% Commit Charge: 145M / 1246M

PCTurboPro - System Performance Warning!

SYSTEM PERFORMANCE WARNING

100 % CPU OVERLOAD

Your CPU usage: 100%

Your PC speed is down. Running programs may freeze and you loose all data.

DANGER LEVEL: HIGH

HELP

● CPU OVERLOAD

NOTICE: you must have a registered version of PCTurboPro to get rid of the problems

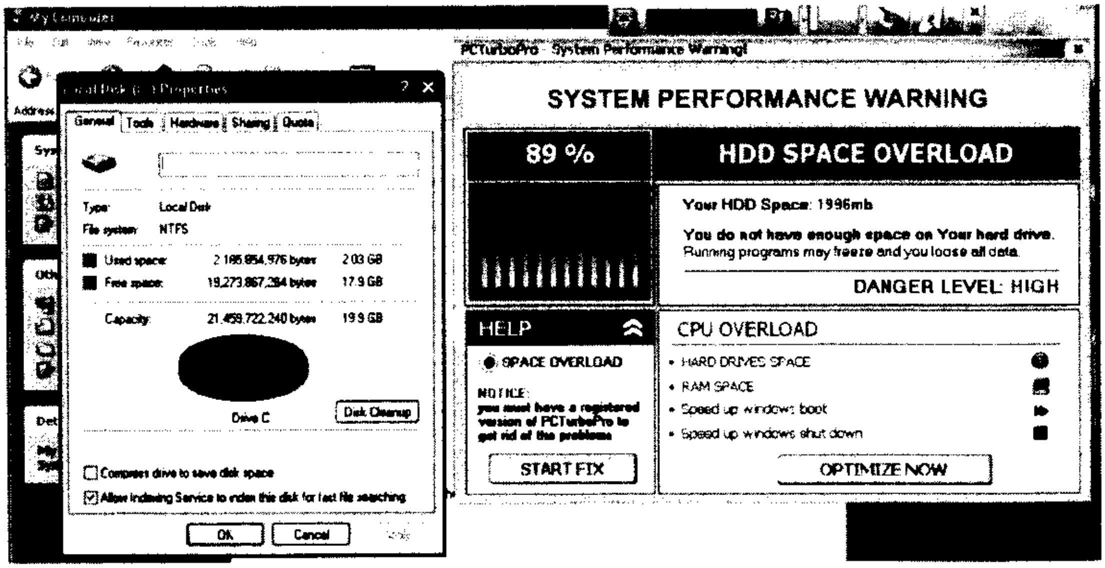
START FIX

CPU OVERLOAD

- HARD DRIVES SPACE
- RAM SPACE
- Speed up windows boot
- Speed up windows shut down

OPTIMIZE NOW

On the right hand side of the screen is the warning from PCTurboPro that states my system is in a "CPU OVERLOAD" state. lt documents that the system is currently running at 100% of the CPU's capabilities. The Windows Task Manager screen to the left shows that this is not only incorrect, it is significantly incorrect.



My Computer

Local Disk (C:) Properties

General | Tools | Hardware | Sharing | Quota

Type: Local Disk

File system: NTFS

Used space:	2 185,854,976 bytes	2.03 GB
Free space:	19,273,867,264 bytes	17.9 GB
Capacity:	21,459,722,240 bytes	19.9 GB

Drive C Disk Cleanup

□ Compress drive to save disk space

☑ Allow Indexing Service to index this disk for fast file searching

OK Cancel Apply

PCTurboPro - System Performance Warning!

SYSTEM PERFORMANCE WARNING

89 % HDD SPACE OVERLOAD

Your HDD Space: 1996mb

You do not have enough space on Your hard drive. Running programs may freeze and you loose all data.

DANGER LEVEL: HIGH

HELP

● SPACE OVERLOAD

NOTICE: you must have a registered version of PCTurboPro to get rid of the problems

START FIX

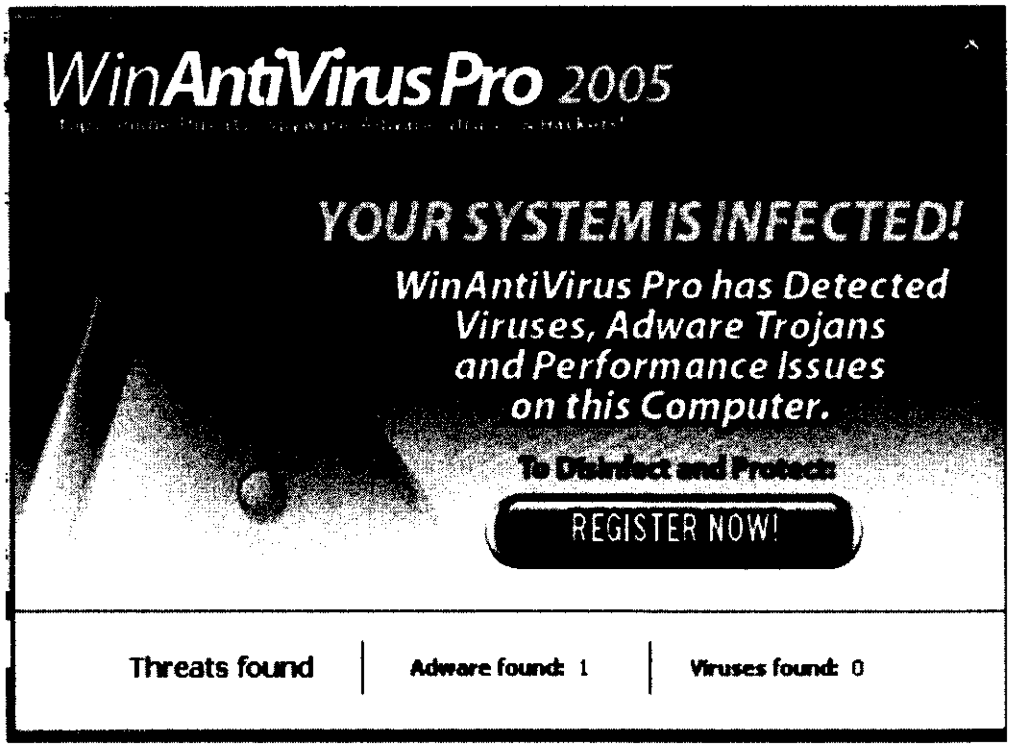
CPU OVERLOAD

- HARD DRIVES SPACE
- RAM SPACE
- Speed up windows boot
- Speed up windows shut down

OPTIMIZE NOW

l also selected the hard disk drive button on the PCTurboPro toolbar and received the above warning, which is on the right. To the left is Windows displaying the properties of the drive. As with the CPU message, PCTurboPro incorrectly alerts the user to a non-existent problem. The hard drive is nowhere near 89% full as reported by PCTurboPro. In my expert opinion, PCTurboPro also uses scare tactics to convince the user they need to purchase the registered version.

Since the Ellis report specifically notes that the WinAntivirus2005ProScannerSetup found 0 items of interest in my original analysis and that the other tools were not antivirus tools so my analysis was invalid, I decided to test WinAntivirus2005ProScannerSetup further. To accomplish this, I used a fresh install of Windows XP SP2, as in my previous analysis. The one exception was that before installing the software package, I browsed to msn.com. I then installed and ran the scanner software. The below warning message was the result.



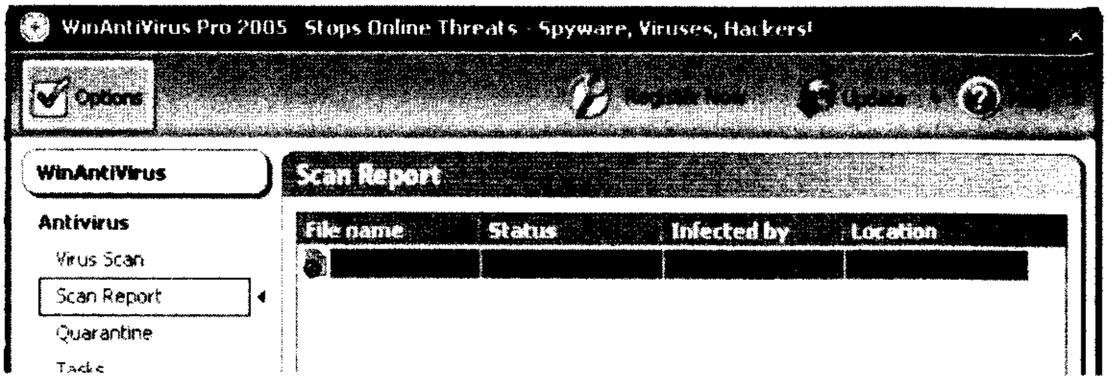
YOUR SYSTEM IS INFECTED!

WinAntiVirus Pro has Detected Viruses, Adware Trojans and Performance Issues on this Computer.

To Disinfect and Protect:

Threats found | Adware found: 1 | Viruses found: 0

This large and scary message states that my "SYSTEM IS INFECTED!" At the bottom of the message we see that the software found one instance of Adware. I would like to point out that the term adware is an industry standard term that is defined by Wikipedia as "*any software package which automatically plays, displays, or downloads advertisements to a computer after the software is installed on it or while the application is being used.*" The key point here is that it refers to a piece of software that performs some action by itself.



WinAntiVirus Pro 2005 Stops Online Threats - Spyware, Viruses, Hackers!

Scan Report

File name	Status	Infected by	Location
[redacted]	[redacted]	[redacted]	[redacted]

As we can see from the results screen above, this *adware* threat is a simple browser cookie, a text file, from the Doubleclick network. This cookie cannot *play, display or download advertisements*. As with the other tools, WinAntiVirus2005ProScannerSetup uses alarmist and false language to scare the user into purchasing the paid version.

To verify that the remaining programs tested by Ellis were the irrelevant paid versions, I extracted the other five pieces of software from the drive image the FTC provided me. As a side note, two of the file names referenced in the Ellis report were incorrect. I found that WinFixer2006PaidSetup.exe was actually WinFixer2006Setup.exe and DriveCleaner2007PaidSetup was actually drivecleaner_setup_07.exe. I was able to determine that these were the same files using the md5 hashes Ellis put into the report. I do not know where the filenames he provided originated. I was able to determine that all of these pieces of software were registered versions and as such are irrelevant to my report.

III. Conclusions

In my expert opinion, my conclusions from the previous report are not changed in the slightest.

First, the graphic files and flash objects do not perform scanning operations. Furthermore after reviewing the code used to load the ads, it is obvious no other scanning was being performed before the advertisement was displayed. These files would confuse the user viewing them into thinking their computer had alerted them to a problem with their system. This would cause them to click the ad.

Second, all of the free versions of the software I have analyzed were designed to lead the user into purchasing the paid version through alerting on either false items or exaggerating the threats of its findings. I further conclude that analyzing the paid versions of this software has no relevance to my analysis.

4-16-10

Kevin Johnson

Date